Sentinel

OTP

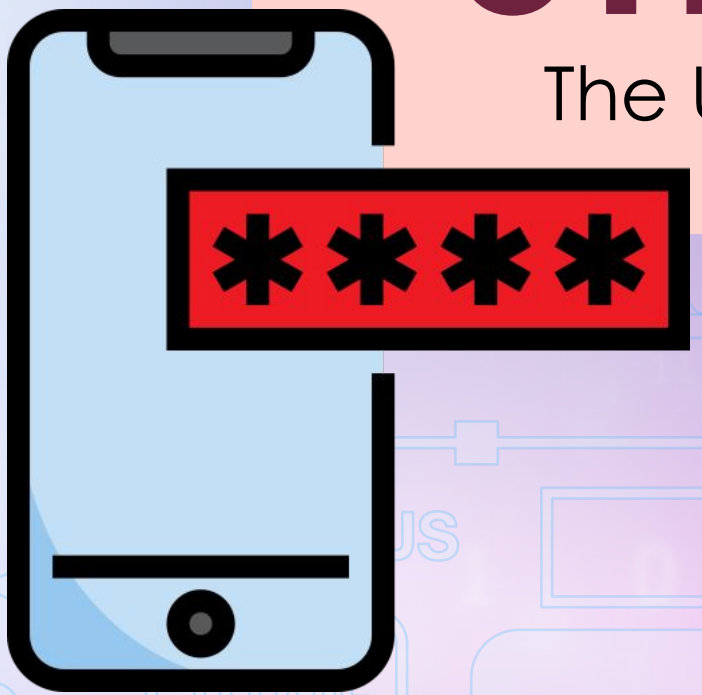
The Unbreakable Cipher

DEFENDING OUR DIGITAL WAY OF LIFE

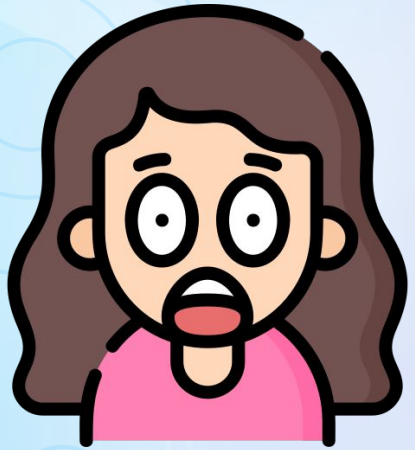
Sentinel

OTP

The Unbreakable Cipher



The Unbreakable Cipher!



What?? How could that be?

Didn't you say that there's no such thing as a totally secure cipher?

Well...

OTP – One Time Pad

The idea is simple. Each party has a copy of the same key

The key has to be at least as long as the encrypted message

Why?

Length

=

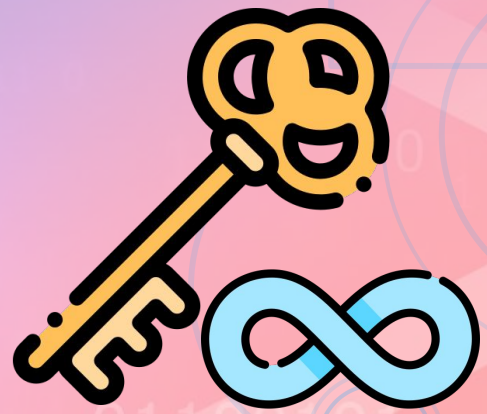
Length

OTP – One Time Pad

Each letter of the message is encoded using a letter of the key

The “used up” parts of the key are never reused

It’s like Vigenère with an infinite key!



OTP – Encrypt Example

"ATTACK AT DAWN"

Key: "SHHDONTTELLANYONE"
Algorithm: **Add** and Modulo 26

A	T	T	A	C	K
S	A	A	D	Q	X

(A + S) % 26
= 0 + 18
= S

(T + H) % 26
= (19 + 7) % 26
= A

OTP – Decrypt Example

"SAADQX TM HLHN"

Key: "SHHDONTTELLANYONE"
Algorithm: **Subtract** and Modulo 26

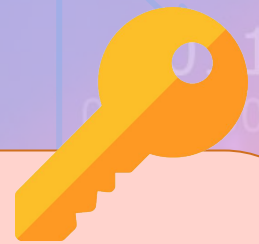
S	A	A	D	Q	X
A	T	T	A	C	K

(S - S) % 26
= 0
= A

(A - H) % 26
= (0 - 7) % 26
= 19
= T

But is it really unbreakable?

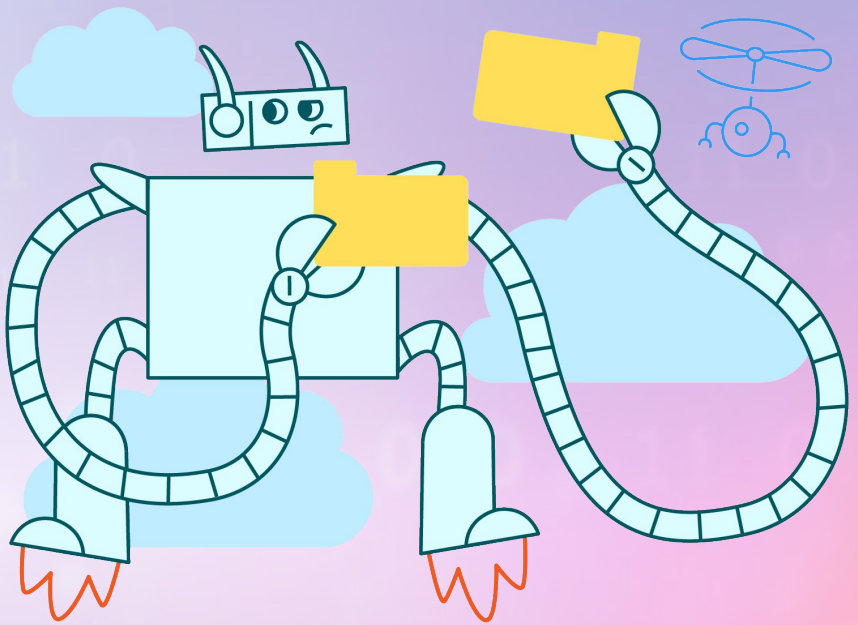
Well… **Yes!** But only if:



1. The key is at least as long as the plaintext
2. The key is completely random
3. The key is never reused in part or completely
4. The key is kept completely secret

OTP Disadvantages?

The main disadvantage is that you need a way to securely communicate a very large key



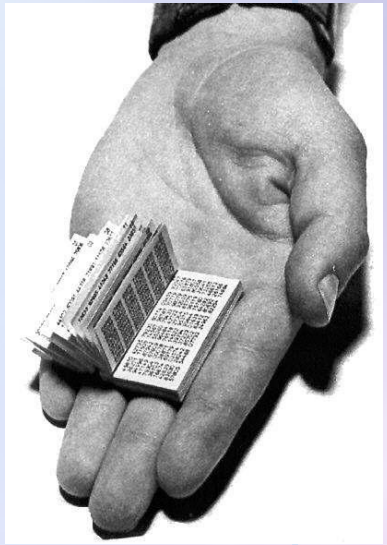
OTP IRL

One Time Pad encryption was used throughout history

The Germans, NSA, Soviets all used OTP to hide their communication from the early 1920s

OTP IRL

Even by 1960, captured KGB spies would still be found with physical one-time pads in their possession

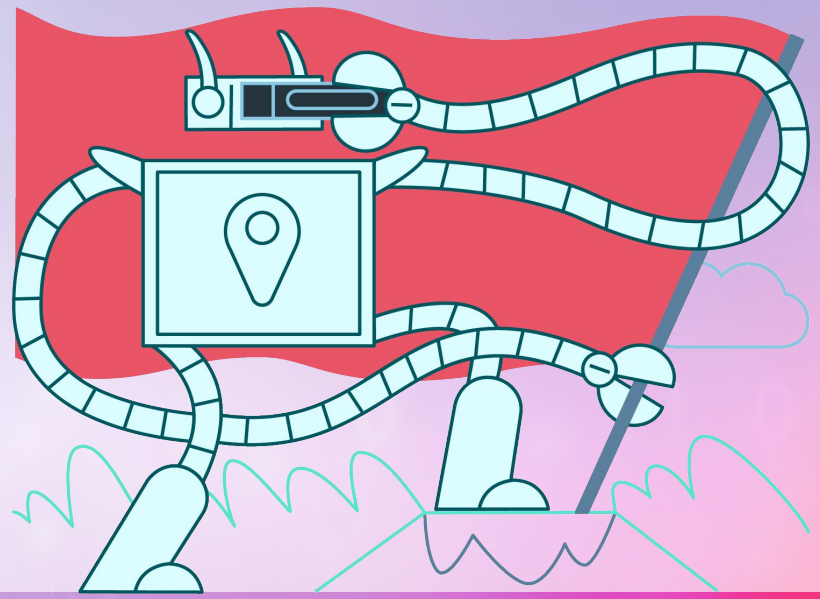


Breaking OTP

Nah...
jk.

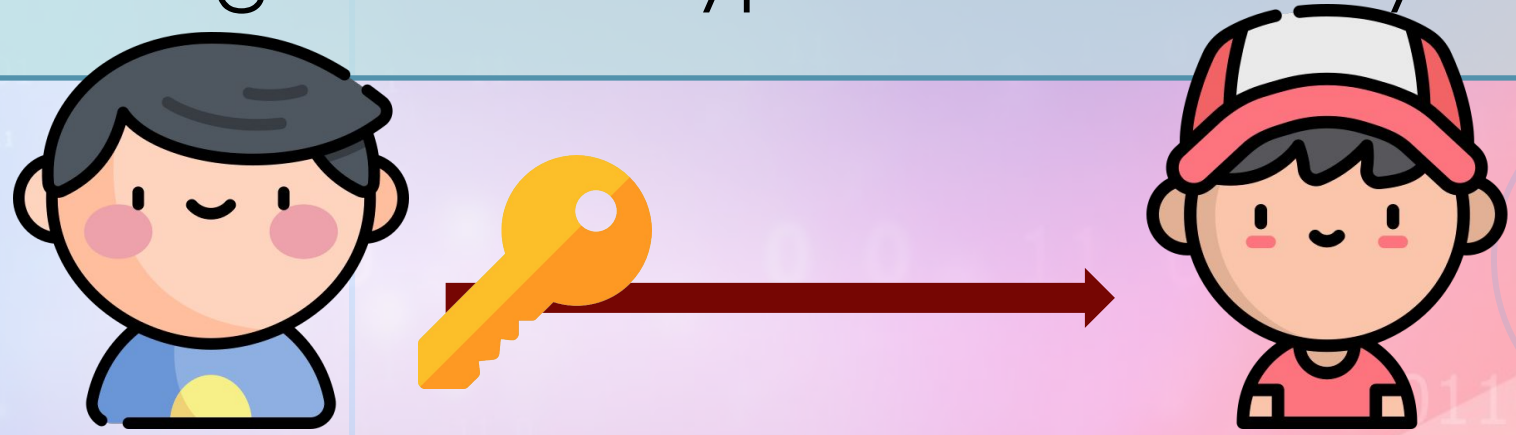
Let's encrypt!

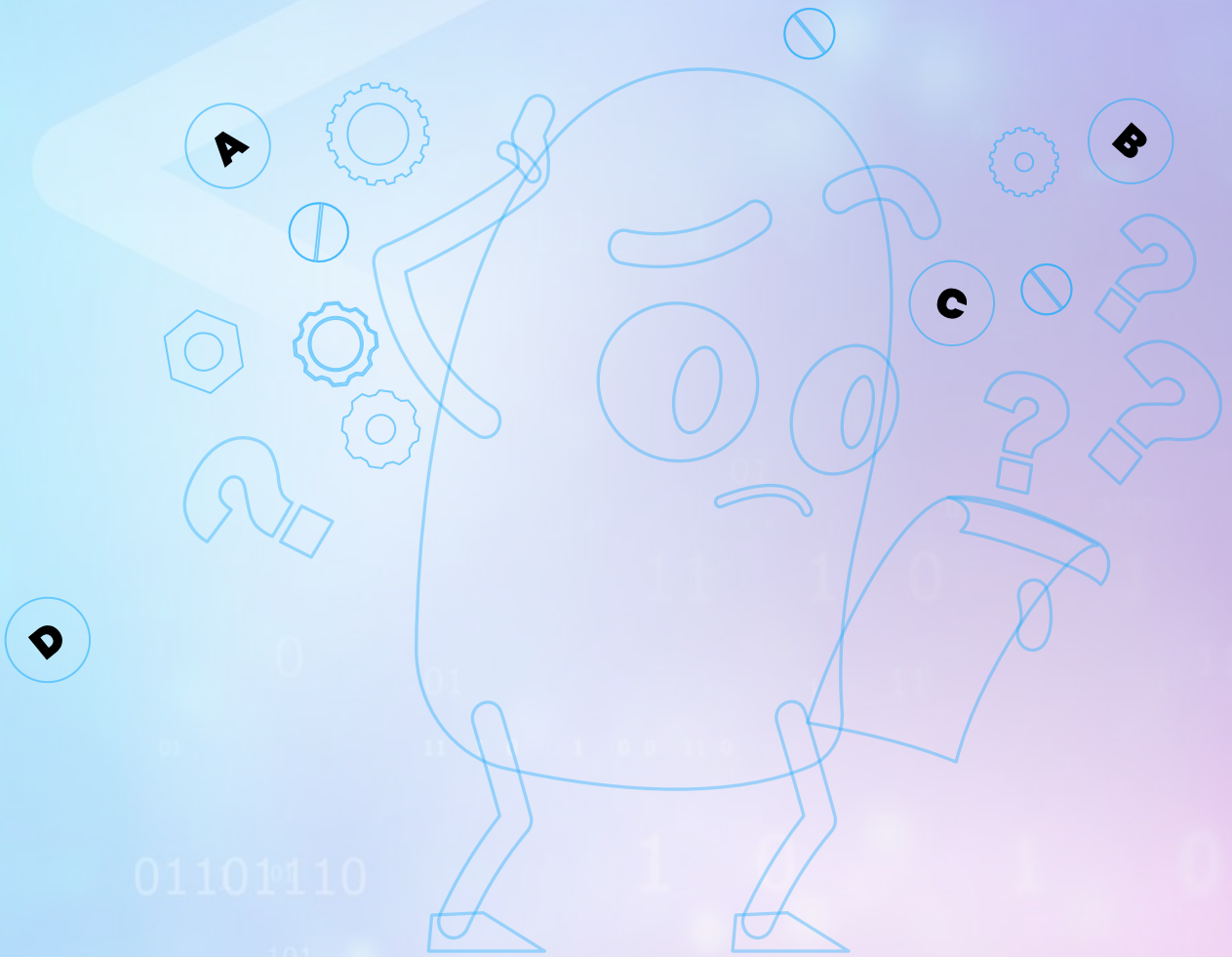
Now you have all the knowledge and tools to implement your own OTP encryptor and decryptor!



Let's encrypt!

1. Write the encryptor and decryptor
2. Encrypt a message
3. Secretly share the key with a friend
4. See if they can decrypt your message using their decryptor and the key





Questions?

Sentinel

Your Turn!

> Play around, have fun, ask questions!